Cyber Defence in the Armed Forces of the Czech Republic

Josef Kaderka, Milan Jirsa
University of Defence
Department of Communication and Information Systems
Kounicova 65
662 10 Brno
Czech Republic

josef.kaderka@unob.cz, milan.jirsa@unob.cz

ABSTRACT

This article briefly describes the state of cyber defence in the Armed Forces of the Czech Republic (Czech Army for short) and some of the problems associated with military and public computer networks interconnecting.

1.0 INTRODUCTION

In the past few years, threats in cyberspace have risen enormously. Securing cyberspace is a difficult task that requires a coordinated effort from entire society – the government, ministries and the private sector. The main goal is to protect against disruption of important information systems forming the critical information infrastructure.

NATO pays attention to cyber threats for a long time. At first, the main effort was focused on the protection of internal military networks, and not the public communications systems. At the 2002 Prague Summit, NATO leaders decided about NATO Cyber Defence Programme implementation. Creation of NATO Computer Incident Response Capability (NCIRC), which task was to strengthen the ability for a rapid response to cyber incidents, was part of this programme. At the same time, NATO member countries stipulated the requirement to establish national CIRC teams.

Massive attack on public and private web sites in Estonia in May 2007 noted the vulnerability of modern society for this type of attack, and stirred debate on whether this particular attack on the NATO member country should not be seen as an attack on the entire alliance according to Article 5 of the Washington Treaty. Finally, it was felt that not, but the work on the conceptual solution to cyber defence within NATO was accelerated.

In order to increase the ability of NATO member states three major documents were issued in early 2008– the NATO Policy on Cyber Defence, NATO Cyber Defence Concept and NATO Cyber Defence Management Authority (CDMA). The documents recommend to Member States the organizational structure and elements of NATO to command a certain action on a coordinated approach to cyber security defence and for the implementation of specific cyber attacks to take appropriate countermeasures.

2.0 CYBER DEFENCE IN THE CZECH ARMY

Several factors influence the solution of cyber defence in the Czech Army. Membership in NATO, fulfilment of NATO obligations, and military aspects of cyber defence are the crucial ones. The European Union, on the other hand, put emphasis on aspects like computer crime, critical infrastructure protection, and, more generally, seek to strengthen the security of and the trust in the information society. And from the national level it is the activity connected with the document National Strategy of Information Security and attempts to use Internet for public administration tasks.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Defence in the Armed Forces of the Czech Republic	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Defence Department of Communication and Information Systems Kounicova 65 662 10 Brno Czech Republic**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
This article briefly describes the state of cyber defence in the Armed Forces of the Czech Republic (Czech Army for short) and some of the problems associated with military and public computer networks interconnecting.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**6**	

Currently there is no comprehensive approach addressing cyber defence in the Czech Republic, nor is it clear the role of the army in any cyber attack on the national critical information infrastructure. It can be said that the army, using the experience and materials of NATO, is in comparison with the civilian community a little bit ahead.

2.1 CIRC of the Czech Army

In January 2007, the CIRC of the Czech Army was established. As a part of this centre the Computer Emergency Readiness Team (CERT) was founded, that serves as a central source of security patches and up to date antivirus databases. CERT also runs a web portal with information, advice and mandatory guidelines for security administrators.

CIRC helps commanders and management in a decision making process, but also to achieve and maintain a secure and reliable information and communication environment in several areas, like:

Operational safety of CIS:

- constitution of general security awareness amid users,
- implementation of CIS security policy,
- defining the rules and how to implement a security audit of hardware and software,
- verifying security audit CIS operators,
- defining and ensuring compliance with software licensing policy used in the CIS.

Active cyber defence of CIS:

- identifying the vulnerability of information systems,
- identifying security threats and incidents, incident and vulnerability handling,
- maintaining the capacity to respond immediately to these incidents,
- monitoring network activity,
- providing opportunities to maintain the individual computers and the entire CIS ready for a potential attack (security patches, updates, virus-sheets, safe settings).

Another CIRC role is to ensure active protection of the communication infrastructure and integrity of data in information systems departmental databases, secure network management with the use of firewalls at the perimeter, including the security of routers, with implementation of IPS (Intrusion Protection System), with the active protection solution for workstations and servers' security of wireless networks. At the same time, it deals with the protection from intruders, viruses and worms, and implements security features. Important task is also security awareness among the military community as a first line of defence for the security of information systems and networks.

3.0 INFORMATION SYSTEM OF DATA BOXES

Serious challenge to military networks security emerged when the Act 300/2008 Coll., on Electronic Actions and Authorized Document Conversion, also known as the "Electronic Actions Act", has been set to take effect as of July 1, 2009. It put into practice the Informative System of Data Boxes, which administrator is the Ministry of Interior and its operator is the Czech Post. It should reduce the number of notices served by personal delivery, simplifying communication between citizens and public authority bodies.

The Act obliged all legal entities and company branch offices registered in the Commercial Register to ensure that there was a computer with an Internet connection in the entity's office and to check their data box regularly.

Since 1 July 2009 all state authorities – from governmental offices, municipal offices, health insurance companies and Czech TV broadcaster to state funds – are obliged to communicate electronically with each other and with certain private sector entities and individuals by using official data boxes.

By the end of September 2009, the Ministry of the Interior set up data boxes for all mentioned authorities, and also for every legal entity and branch office registered in the Commercial Register. Other legal entities, individual entrepreneurs and citizens can apply to the Ministry for their own data box, which will be set up within three days of submitting the application. Hence ordinary citizens are not obliged to have their own data boxes.

3.1 Security and Legal Position

Public authority bodies are now obliged to correspond electronically with all entities that have established a data box. The Civil Procedure Act has been amended to take this into account, and specifies the correct priority order that the court must use when attempting to deliver correspondence to an entity. First, the court must attempt to deliver correspondence during hearings or other court actions, but if this is impossible, the court must deliver correspondence to the data box. If delivery to the data box is impossible (e.g. the recipient is an individual for whom no data box has been set up), then the court will deliver correspondence to the physical or e-mail address provided by the recipient during the proceedings. As a last resort, the court will physically deliver correspondence to the registered permanent residence of an individual or the registered office of an entity.

Under the Electronic Actions Act, a data box may only be accessed by the person for whom it has been created or a representative appointed by that person for this purpose. Access to a legal entity's data box is provided to the entity's statutory body or its members, who may then authorize other individuals to access the data box. The data box username and password is delivered to the user by registered mail immediately after the data box has been set up. The data box is activated after the authorized user first logs in to the data box system. Automatic activation will take place if there is no login within 15 days after the data box has been set up.

The entire data box system cannot be regarded as classic e-mail boxes. It is a proprietary solution, and it works in a secure and guaranteed way. Any messages sent from a data box is provided with a time stamp and electronic mark (which is analogous to a guaranteed electronic signature), with all attachments time-stamped and marked accordingly. The system then delivers the message to its recipient and generates a receipt informing the sender, whether the message was delivered and when it was read. However, the data box system uses the same security level as ordinary e-mail, because only the username and password are required to access a data box.

Documents sent to a data box are legally deemed delivered as soon as the authorized user logs in, after which point it will be assumed that the recipient has become familiar with the document. A document will be deemed to have been delivered and received by the recipient 10 days after it was sent, even if the user has not accessed the data box, unless the law expressly specifies that presumption of delivery does not apply, for example, in the event of the delivery of a summons to a preliminary hearing or the delivery of a payment order in accordance with the Civil Procedure Act.

The delivery of documents to a data box through the public data network is considered to be a type of personal delivery. Legal entities and individuals alike had to activate their data boxes as soon as they received the login details and check for updates regularly. This helped to avoid any unpleasant surprises – obligations arising from legitimate governmental decisions left unread in an overflowing data box.

3.2 Experience with Data Boxes

The first experience with the Informative System of Data Boxes is surprisingly good. There were some minor questions, but their number was much lower than calamity-howlers anticipated, and they were solved very promptly.

4.0 PROPOSED SOLUTION

The Czech Army operates several data networks. Their internal structure, interconnections and security elements placement are relatively complicated. The relevant simplified conceptual scheme is depicted in the Figure 1.

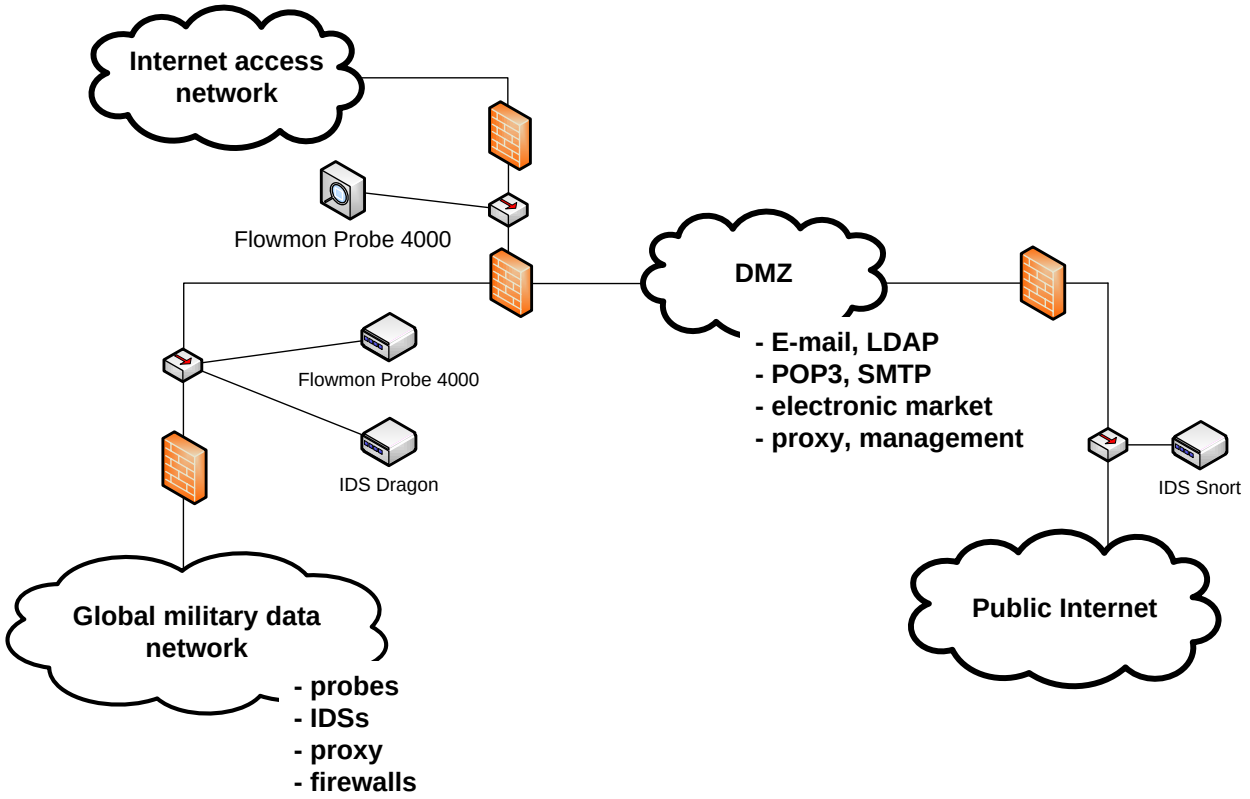

Figure 1: Conceptual Schema

The global military data network is the largest one, it serves as communication environment for several information systems, voice services etc., this network is not secured. That network was significantly upgraded last year and the backbone bandwidth is now typically 465 Mbps. The separated Internet access network provides Internet sources and services access for the military users.

As it was already mentioned, the CIRC plays an important role in the Czech Army overall and especially in computer network security. It is mainly focused on security monitoring, rather than routine traffic monitoring.

In order to implement this monitoring, it was necessary to select appropriate technologies and tools. It should be noted that the selection process is not simple and is still ongoing, never ending respectively. Many solutions have been gradually verified, each of them has its weaknesses and strengths. An example includes Cisco Mars, Enterasys Dragon and many others.

Relatively unusual solution has been used in order to perform quality monitoring with the possibility of the undesirable action backward discovery. This solution is based on special tools using NetFlow protocol. Active network elements or specialized hardware probes attached to the backbone network using a tap can be the sources of NetFlow data. The principal advantage of NetFlow protocol is the fact that it provides primary data in the open form, which can be easily utilized in the subsequent operations. The FlowMon Probe 4000 is mostly used NetFlow probe, it consists of two 10/100/1000 Mbps Ethernet monitoring ports as default. The manufacturer is INVEA-TECH, a university spin-off company devoted to the development of state-of-the-art solutions for high-speed network applications.

5.0 CONCLUSIONS

The security of the data networks is big challenge. The Czech Army upgraded its data network lately and gradually moves more services from the classical systems to the IP platform. It is a significant quality shift and it needs true field and security specialists in the first raw. The national CIRC team has been established to improve security according NATO recommendation. CIRC has got good reputation during its short existence. New solutions like Information Systems of Data Boxes represents new needs, sometimes in violation with long term habits.

6.0 REFERENCES

[1] Conceptual documents of MoD cyber defence working group. Non-public material. 2009.

[2] Official homepage of Data boxes. [online]. http://www.datoveschranky.info

[3] TVRDÁ, Markéta. Data boxes: official notices in the digital revolution. [online]. http://www.businessinfo.cz/en/article/czech-republic-business-news/official-notices-in-digital-revolution/1001536/53778